WHAT IS CLAIMED IS:

1. A communication system including:

a transmitter;

a receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol;

at least one TMDS-like link coupled between the transmitter and the receiver, wherein the transmitter is operable in an encryption mode in which it generates encrypted data by encrypting first data using a secret value and transmits the encrypted data over the at least one TMDS-like link to the receiver, and the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using the secret value; and

an external agent configured to be coupled to the receiver and to the transmitter, wherein the receiver is configured to send a ticket request to the external agent when the receiver is coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and to send signals to the transmitter and the receiver in response to each granted request to enable the transmitter and the receiver to operate in the encryption mode and the decryption mode respectively, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter and the receiver to obtain the secret value.

2. The system of claim 1, also including:

a second TMDS-like link coupled to the receiver, wherein the receiver is a repeater coupled to receive the encrypted data from the transmitter and configured to generate translated data by processing the decrypted data, to generate re-encrypted data by encrypting the translated data, and to transmit the re-encrypted data over the second TMDS-like link; and

a second receiver coupled to the second TMDS-like link, wherein the second receiver is configured to receive the re-encrypted data transmitted from the translating router and to decrypt the re-encrypted data.

3. The system of claim 1, also including a router, wherein the at least one TMDS-like link includes a first TMDS-like link coupled between the transmitter and the router, and a second TMDS-like link coupled between the router and the receiver,

wherein the router is coupled to receive the encrypted data from the transmitter and to forward the encrypted data over the second TMDS-like link to the receiver.

4. The system of claim 1, wherein the transmitter is a repeater, and the system also includes:

a content source; and

a serial link between the content source and the repeater, wherein the content source and the repeater are configured to implement a second content protection protocol according to which the content source transmits second encrypted data over the serial link to the repeater, the content source is operable in an encryption mode in which it generates the second encrypted data by encrypting input data using a second secret value, and the repeater is operable in a second decryption mode in which it generates the first data from the second encrypted data including by decrypting the second encrypted data using the second secret value.

5. The system of claim 4, wherein the repeater is configured to send a second ticket request to the external agent when the repeater is coupled to the external agent, and the external agent is configured to respond to the second ticket request by determining or obtaining a determination as to whether to grant the second ticket request, and sending second signals to the content source and the repeater in response to each granted second ticket request, wherein the second signals include at least one of the second secret value, an encrypted version of the second secret value, and data enabling the content source and the repeater to obtain the second secret value.

6. The system of claim 4, wherein the content protection protocol is an AES protocol and the second content protection protocol is an HDCP protocol.

7. The system of claim 4, wherein each of the content protection protocol and the second content protection protocol is an AES protocol.

8. The system of claim 4, wherein the content protection protocol is a symmetric content protection protocol.

9. The system of claim 1, also including a switch, wherein the at least one TMDS-like link includes a first TMDS-like link coupled between the transmitter and the switch, a second TMDS-like link coupled between the switch and the receiver, and a third TMDS-like link, wherein the switch is coupled to receive the encrypted data from the transmitter and to assert the encrypted data over a selected one of the second TMDS-like link and the third TMDS-like link.

10. The system of claim 1, wherein the external agent is configured to verify the identity of at least one of the receiver and transmitter including by examining a cryptographically secure digital signature.

11. The system of claim 1, wherein the transmitter is operable in the encryption mode to generate the encrypted data by encrypting the first data using a sequence of secret values including the secret value, and to transmit the encrypted data over the at least one TMDS-like link to the receiver, and the receiver is operable in the decryption mode to generate the decrypted data by decrypting the encrypted data using the sequence of secret values.

12. A communication system including:

a transmitter;

a router;

a receiver configured to implement a content protection protocol and a second content protection protocol;

at least one serial link coupled between the transmitter and the router;

at least one additional serial link coupled between the router and the receiver, wherein the router and the receiver are operable in at least one of a first mode and a second mode, wherein, in the first mode, the router forwards to the at least one additional serial link multiply encrypted data received from the at least one serial link, and the receiver generates encrypted data by decrypting the multiply encrypted data using a secret value in accordance with a first content protection protocol, and

wherein, in the second mode, the router generates encrypted data by performing a translation operation on multiply encrypted data received from the at least one serial link, wherein the translation operation includes decryption of the multiply encrypted data using a second secret value in accordance with a second content protection protocol, the router forwards the encrypted data to the at least one additional serial link, and the receiver generates decrypted data by decrypting the encrypted data received from the at least one additional serial link in accordance with the second content protection protocol using a third secret value; and

an external agent configured to be coupled to at least one of the transmitter, the router, and the receiver, wherein said at least one of the transmitter, the router, and the receiver is configured to send a ticket request to the external agent when coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending signals to at least one of the transmitter, the router, and the receiver in response to each granted request to enable the router and the receiver to operate in at least one of the first mode and the second mode, wherein the signals include at least one of the secret value, the second secret value, the third secret value, an encrypted version of the secret value, an encrypted version of the second secret value, an encrypted version of the third secret value, data enabling the receiver to obtain the secret value, data enabling the router to obtain the second secret value, and data enabling the receiver to obtain the third secret value.

13. The system of claim 12, wherein the second secret value is identical to the third secret value.

14. The system of claim 12, wherein the at least one additional serial link is a TMDS-like link coupled between the router and the receiver.

15. The system of claim 12, wherein the receiver is configured to send the ticket request to the external agent when said receiver is coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending at least one signal to the receiver in response to grant of the request to enable the receiver to operate in said at least one of the first mode and the second mode, wherein the at least one signal includes at least one of the secret value, the third secret value, the encrypted version of the secret value, the encrypted version of the third secret value, the data enabling the receiver to obtain the secret value, and the data enabling the receiver to obtain the third secret value.

16. A communication system including:

a transmitter;

a translating router;

a receiver, wherein the transmitter and the translating router are configured to implement a content protection protocol, and the translating router and the receiver are configured to implement a second content protection protocol;

a first link between the transmitter and the translating router, and second link between the translating router and the receiver, wherein at least one of the first link and the second link is a TMDS-like link, wherein the transmitter is configured to generate encrypted data by encrypting first data using a secret value and transmit the encrypted data over the first link to the translating router, the translating router is configured to generate decrypted data by decrypting the encrypted data using the secret value, to generate translated data by processing the decrypted data, to generate re-encrypted data by encrypting the translated data using a second secret value, and to transmit the re-encrypted data over the second link, and the receiver is configured to generate additional decrypted data by decrypting the re-encrypted data using the second secret value; and

an external agent configured to be coupled to each of at least two of the receiver, the translating router, and the transmitter, and to perform at least one function essential to implementation of at least one of the content protection protocol and the second content protection protocol.

17. The system of claim 16, wherein the translating router is configured to send a ticket request to the external agent when the translating router is coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending signals to the translating router and the transmitter in response to each granted request, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the translating router and the transmitter to obtain the secret value.

18. The system of claim 17, wherein the receiver is configured to send a second ticket request to the external agent when the receiver is coupled to the external agent,

and the external agent is configured to respond to the second ticket request by determining or obtaining a determination as to whether to grant the second ticket request, and sending second signals to the translating router and the receiver in response to each granted second ticket request, wherein the second signals include at least one of the second secret value, an encrypted version of the second secret value, and data enabling the translating router and the receiver to obtain the second secret value.

19. The system of claim 16, wherein the receiver is configured to send a ticket request to the external agent when the receiver is coupled to the external agent, and the external agent is configured to respond to the ticket request by determining or obtaining a determination as to whether to grant the request, and sending signals to the translating router and the receiver in response to each granted request, wherein the signals include at least one of the second secret value, an encrypted version of the second secret value, and data enabling the translating router and the receiver to obtain the second secret value.

20. The system of claim 16, wherein each of the content protection protocol and the second content protection protocol is a symmetric content protection protocol.

21. A communication system including:

a transmitter;

a repeater;

a receiver, wherein the transmitter and the repeater are configured to implement a content protection protocol, and the repeater and the receiver are configured to implement a second content protection protocol;

a first link between the transmitter and the repeater, and second link between the repeater and the receiver, wherein at least one of the first link and the second link is a TMDS-like link, wherein the transmitter is configured to generate encrypted data by encrypting first data using a secret value and transmit the encrypted data over the first link to the repeater, the repeater is configured to generate decrypted data including by decrypting the encrypted data using the secret value, to generate re-encrypted data including by encrypting the decrypted data using a second secret value, and to transmit the re-encrypted data over the second link, and the receiver is configured to generate additional decrypted data by decrypting the re-encrypted data using the second secret value; and

an external agent, configured to be coupled to each of at least two of the receiver, the repeater, and the transmitter, and to perform at least one function essential to implementation of at least one of the content protection protocol and the second content protection protocol.

22. The system of claim 21, wherein the repeater is configured to send a ticket request to the external agent when the repeater is coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending signals to the repeater and the transmitter in response to each granted request, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the repeater and the transmitter to obtain the secret value.

23. The system of claim 21, wherein the receiver is configured to send a second ticket request to the external agent when the receiver is coupled to the external agent, and the external agent is configured to respond to the second ticket request by determining or obtaining a determination as to whether to grant the second ticket request, and sending second signals to the repeater and the receiver in response to each granted second ticket request, wherein the second signals include at least one of the second secret value, an encrypted version of the second secret value, and data enabling the repeater and the receiver to obtain the second secret value.

24. The system of claim 21, wherein the receiver is configured to send a ticket request to the external agent when the receiver is coupled to the external agent, and the external agent is configured to respond to the ticket request by determining or obtaining a determination as to whether to grant the request, and sending signals to the repeater and the receiver in response to each granted request, wherein the signals include at least one of the second secret value, an encrypted version of the second secret value, and data enabling the repeater and the receiver to obtain the second secret value.

25. The system of claim 21, wherein the repeater is configured to send a ticket request to the external agent when the repeater is coupled to the external agent, wherein

the request is on behalf of the repeater and the receiver, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending signals to at least one of the repeater and the receiver in response to each granted request, wherein the signals include at least one of the secret value and the second secret value, encrypted versions of the secret value and the second secret value, and data enabling the repeater to obtain the secret value and the second secret value and the receiver to obtain the second secret value.

26. The system of claim 21, wherein the second content protection protocol is a symmetric content protection protocol.

27. The system of claim 26, wherein the second link is a TMDS-like link, the content protection protocol is an AES protocol and the symmetric content protection protocol is an HDCP protocol.

28. The system of claim 26, wherein the second link is a TMDS-like link, and the symmetric content protection protocol is a modified HDCP protocol which requires that the repeater and the receiver obtain the second secret value directly or indirectly from the external agent.

29. The system of claim 21, wherein the second link is a TMDS-like link, and each of the content protection protocol and the second content protection protocol is an AES protocol.

30. The system of claim 29, wherein the second content protection protocol is an AES-128 CTR protocol.

31. A communication system including:

a transmitter;

a receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol;

at least one TMDS-like link coupled between the transmitter and the receiver, wherein the transmitter is operable in an encryption mode in which it generates encrypted data by encrypting first data using a secret value and transmits the encrypted data over the at least one TMDS-like link to the receiver, and the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using the secret value; and

an external agent configured to be coupled to the receiver and to the transmitter, wherein at least one of the receiver and the transmitter is configured to send a ticket request to the external agent when coupled to the external agent, the request includes data indicative of at least one capability of the receiver, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending signals to at least one of the transmitter and the receiver in response to each granted request to enable the transmitter and the receiver to operate in the encryption mode and the decryption mode respectively.

32. The system of claim 31, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter and the receiver to obtain the secret value.

33. The system of claim 31, wherein the data indicative of at least one capability of the receiver indicates whether the receiver can assert unprotected digital data at an output of said receiver.

34. The system of claim 31, wherein the data indicative of at least one capability of the receiver indicates whether the receiver can assert digital data protected by a content protection protocol at an output of said receiver.

35. The system of claim 31, wherein the external agent is configured to verify the identity of at least one of the receiver and transmitter including by examining a cryptographically secure digital signature.

36. A communication system including:

a transmitter;

a receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol;

a serial link coupled between the transmitter and the receiver, wherein the transmitter is operable in an encryption mode in which it generates encrypted data and transmits the encrypted data over the link to the receiver, and the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using a key; and

an external agent configured to be coupled to the receiver and to the transmitter, wherein at least one of the receiver and the transmitter is configured to send a ticket request to the external agent when coupled to the external agent, and the external agent is configured to respond to the request by determining or obtaining a determination as to whether to grant the request, and sending at least one signal to one of the transmitter and the receiver in response to each granted request, wherein the at least one signal is indicative of data that determines a pre-encrypted version of the key and data enabling the receiver to decrypt the pre-encrypted version of the key.

37. A communication system including:

a transmitter including a cipher engine;

a receiver including a second cipher engine; and

a serial link coupled between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a symmetric block protocol in which the transmitter sends encrypted data over the link to the receiver, and the second cipher engine decrypts the encrypted data in response to a key and a sequence of count values, wherein the cipher engine is configured to generate a randomizer value, the transmitter is configured to transmit the randomizer value to the receiver, and the receiver is configured to include the randomizer value as a field of at least one of the count values.

38. The system of claim 37, wherein the randomizer value is a pseudo-random value.

39. The system of claim 38, wherein the second cipher engine is configured to decrypt the encrypted data in response to the sequence of count values and a sequence of keys including said key, the cipher engine is configured to generate a sequence of pseudo-random values including the pseudo-random value, the transmitter is configured to transmit the sequence of pseudo-random values to the receiver, and the receiver is configured to include each pseudo-random value of the sequence of pseudo-random values as a field of a different one of the count values.

40. The system of claim 37, wherein the serial link is a TMDS-like link including at least one encrypted data transmission channel and a communication channel, and the transmitter is configured to transmit the randomizer value over the communication channel to the receiver .

41. A cipher engine for use in a receiver of a communication system, wherein the system includes a transmitter having a cipher engine and a serial link coupled to the transmitter, the receiver is configured to be coupled to the serial link to receive encrypted data transmitted over the serial link from the transmitter, and the receiver is configured to be coupled to receive a pseudo-random value from the transmitter, said cipher engine including:

counter circuitry configured to generate a sequence of count values, wherein each of the count values has a field determined by the pseudo-random value value; and

a block cipher, coupled to receive a key and coupled to the counter circuitry to receive each of at least a subset of the count values, and configured to generate a pseudo-random output value, for use in decrypting the encrypted data, in response to the key and each of the count values received from the counter circuitry.

42. A cipher engine configured to implement a symmetric block protocol, said cipher engine including:

counter circuitry configured to generate a sequence of count values; and

a block cipher, coupled to receive a sequence of keys, coupled to the counter circuitry to receive each of at least a subset of the count values, and configured to generate a sequence of pseudo-random output values in response to the count values received from the counter circuitry and the keys, wherein the block cipher is configured to generate each of a first subset of the pseudo-random output values by performing X rounds of a cipher algorithm and to generate each of a second subset of the pseudo-random output values by performing Y rounds of the cipher algorithm, where X is an integer and Y is an integer greater than X.

43. The cipher engine of claim 42, wherein the first subset of the pseudo-random output values but not the second subset of the pseudo-random output values is for use in decrypting blocks of encrypted video data, and each of the pseudo-random

output values in the first subset is sufficient for decrypting a block of Z pixels of the encrypted video data, where Z is an integer.

44. The cipher engine of claim 43, wherein the symmetric block protocol is the AES-128 CTR protocol, and wherein X = 5, Y = 10, and Z = 5.

45. The cipher engine of claim 43, wherein the symmetric block protocol is the AES-128 CTR protocol, the block cipher operates in response to a pixel clock, the block cipher is configured such that no more than one cycle of the pixel clock is required to perform each of the rounds of the cipher algorithm, and Z = 5.

46. The cipher engine of claim 42, wherein the block cipher is configured:

to generate an initial pseudo-random output value by performing rounds of a cipher algorithm in response to an initial one of the count values received from the counter circuitry and one of the keys,

to include at least a subset of bits of the initial pseudo-random value as a field of a subsequent one of the count values, and then

to generate a sequence of the first subset of the pseudo-random output values by performing rounds of the cipher algorithm in response to at least one of: said subsequent one of the count values and an incremented version of said subsequent one of the count values.

47. The cipher engine of claim 46, also including a register, and wherein the cipher engine is configured to cause the block cipher to write to the register at least some of the bits of the initial pseudo-random value.

48. The cipher engine of claim 42, also including:

double buffering circuitry coupled to the block cipher, wherein the double buffering circuitry is configured to hold at least two keys of the sequence of keys and to assert either one of said two keys to the block cipher, whereby the block cipher can employ one of the keys held in the double buffering circuitry to generate a subset of the pseudo-random output values while another key is written to the double buffering circuitry or another one of the keys held in the double buffering circuitry is decoded or verified.

49. A communication system, comprising:

a transmitter and a receiver, each of the transmitter and the receiver including a cipher engine; and

a serial link coupled between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a symmetric block protocol in which the transmitter sends encrypted video data over the link to the receiver, and the cipher engine of the receiver decrypts the encrypted video data in response to a sequence of keys and a sequence of count values, wherein the cipher engine of the receiver includes:

counter circuitry configured to generate the sequence of count values; and

a block cipher, coupled to receive the sequence of keys, coupled to the counter circuitry to receive each of at least a subset of the count values, and configured to generate a sequence of pseudo-random output values in response to the count values received from the counter circuitry and the keys, wherein the block cipher is configured to generate each of a first subset of the pseudo-random output values by performing X rounds of a cipher algorithm and each of a second subset of the pseudo-random output values by performing Y rounds of the cipher algorithm, where X is an integer and Y is an integer greater than X.

50. The system of claim 49, wherein the first subset of the pseudo-random output values but not the second subset of the pseudo-random output values is for use in decrypting blocks of the encrypted video data, and each of the pseudo-random output values in the first subset is sufficient for decrypting a block of Z pixels of the encrypted video data, where Z is an integer.

51. The system of claim 50, wherein the symmetric block protocol is the AES-128 CTR protocol, and wherein X = 5, Y = 10, and Z = 5.

52. The system of claim 50, wherein the symmetric block protocol is the AES-128 CTR protocol, the block cipher operates in response to a pixel clock, the block cipher is configured such that no more than one cycle of the pixel clock is required to perform each of the rounds of the cipher algorithm, and Z = 5.

53. A communication system including:

a transmitter;

a receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol;

at least one TMDS-like link coupled between the transmitter and the receiver, wherein the transmitter is operable in an encryption mode in which it generates encrypted data by encrypting first data using a secret value and transmits the encrypted data over the at least one TMDS-like link to the receiver, and the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using the secret value; and

an external agent configured to be coupled to the receiver and to the transmitter, wherein the external agent is configured to operate in a mode in which it sends at least one signal to the receiver and at least one additional signal to the transmitter,

wherein the at least one additional signal is indicative of at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter to obtain the secret value, and

wherein the at least one signal is indicative of first data and second data, wherein the first data comprise at least one of the secret value, an encrypted version of the secret value, and data enabling the receiver to obtain the secret value, the second data includes a code value that identifies the secret key without revealing the secret key, and the secret key cannot be derived from the second data.

54. The system of claim 53, wherein the code value is a key sequence code value.

55. The system of claim 53, wherein the transmitter is configured to access the code value, and to process the code value to determine whether the secret key obtained by the receiver has a correct value.

56. The system of claim 53, wherein the content protection protocol is a symmetric content protection protocol.

57. A communication system including:

a transmitter;

a receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol;

at least one TMDS-like link coupled between the transmitter and the receiver, wherein the transmitter is operable in an encryption mode in which it generates encrypted data by encrypting first data using a secret value and transmits the encrypted data over the at least one TMDS-like link to the receiver, and the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data using the secret value; and

an external agent configured to be coupled to the receiver and to the transmitter, wherein the external agent is configured to operate in a mode in which it sends signals to the transmitter and the receiver, wherein the signals include at least one of the secret value, an encrypted version of the secret value, and data enabling the transmitter and the receiver to obtain the secret value,

and wherein the external agent is also operable in a second mode in which it sends a control signal to the transmitter and a second control signal to the receiver, wherein the transmitter is configured to operate in a pass-through mode in response to the control signal and the receiver is configured to operate in a non-decrypting mode in response to the second control signal, wherein,

in the pass-through mode, the transmitter receives data from a source and transmits the data over the at least one TMDS-like link to the receiver without encrypting said data, and

in the non-decrypting mode, the receiver does not decrypt the data that it receives from the transmitter over the at least one TMDS-like link.

58. A cipher engine, including:

control circuitry configured be coupled to a TMDS-like link to receive a synchronization signal from said link; and

circuitry, coupled to receive a stream of data having active data periods separated by blanking intervals, and configured to perform at least one of an encryption operation and a decryption operation on the data in response to a control signal from the control circuitry,

wherein the control circuitry generates the control signal in response to the synchronization signal, the synchronization signal is received in one of the blanking intervals, the synchronization signal is indicative of a sequence of code words, and the control circuitry is configured to determine a value of the synchronization signal from the number of code words in the sequence.

59. The cipher engine of claim 58, wherein the sequence of code words comprises N code words, where N is an integer, and the control circuitry is configured to determine said value of the synchronization signal by determining whether N has a value in a predetermined range.

60. The cipher engine of claim 59, wherein the control circuitry is configured to recognize the synchronization signal as a key change signal by determining that N has a value in said predetermined range.

61. The cipher engine of claim 58, wherein the sequence of code words comprises N code words, where N is an integer, and the control circuitry is configured to determine said value of the synchronization signal by determining whether N satisfies $L < N < M$, where L is an integer, M is an integer greater than L, $(M – L) = kN$, and k is a predetermined proportionality constant.

62. The cipher engine of claim 61, wherein the control circuitry is configured to recognize the synchronization signal as a key change signal by determining that N satisfies $L < N < M$.

63. A cipher engine configured to implement a symmetric block protocol, said cipher engine including:

control circuitry configured be coupled to a TMDS-like link to receive at least a first control signal and a second control signal from said link;

counter circuitry coupled to the control circuitry and configured to generate a sequence of count values under control of the control circuitry; and

a block cipher, coupled to receive a sequence of keys, coupled to the control circuitry, and coupled to the counter circuitry to receive each of at least a subset of the count values, and configured to generate a sequence of pseudo-random output values in response to the count values received from the counter circuitry and the keys,

wherein the control circuitry is configured to trigger initialization of the counter circuitry in response to the first control signal, and the control circuitry is configured to respond to the second control signal by causing the block cipher to accept the next one of the keys.

64. A communication system including:

a transmitter;

a receiver; and

a serial link coupled between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a symmetric block content protection protocol, the transmitter is operable in an encryption mode in which it generates encrypted data and transmits the encrypted data over the link to the receiver, the receiver is operable in a decryption mode in which it generates decrypted data by decrypting the encrypted data, and each of the transmitter and the receiver includes a cipher engine that implements the protocol, each said cipher engine including:

counter circuitry configured to generate a sequence of count values;

a register; and

a block cipher coupled to receive a sequence of keys, and coupled to the counter circuitry to receive each of at least a subset of the count values, wherein the cipher engine is configured to cause the block cipher to generate an initial pseudo-random output value by performing rounds of a cipher algorithm in response to an initial one of the count values received from the counter circuitry and one of the keys, and to write at least a subset of bits of the initial pseudo-random value to the register, wherein said subset of bits determines a link integrity value, and wherein

the transmitter is configured to perform a link integrity check, by accessing the link integrity value in the register of the receiver's cipher engine and processing said link integrity value with the link integrity value in the register of the transmitter's cipher engine.

65. A translating router, including:

decryption circuitry, configured to be coupled to a first serial link and to generate decrypted data from encrypted data received over the first serial link in accordance with a content protection protocol;

translation circuitry coupled to the decryption circuitry and configured to generate translated data by processing the decrypted data; and encryption circuitry coupled to the translation circuitry, and configured to generate re-encrypted data from the translated data, in accordance with a second content protection protocol, and to assert the re-encrypted data to the second serial link.

66. The translating router of claim 65, wherein the at least one of the first serial link and the second serial link is a TMDS-like link.

67. The translating router of claim 65, wherein the second symmetric content protection protocol is different than the symmetric content protection protocol.

68. The translating router of claim 65, wherein the second symmetric content protection protocol is identical to the symmetric content protection protocol.

69. The translating router of claim 65, wherein at least one of the content protection protocol and the second symmetric content protection protocol is a symmetric content protection protocol.

70. A communication system including:

a transmitter;

a receiver; and

a communication channel between the transmitter and the receiver, wherein the transmitter and the receiver are configured to implement a content protection protocol that includes a procedure for supplying a receiver key to the receiver, and a challenge-response procedure for verifying whether the transmitter has a transmitter key matching the receiver key,

wherein the receiver is configured to encrypt first data in accordance with the protocol using the receiver key to generate an authentication message, and to send the authentication message to the transmitter over the channel, the transmitter is configured to perform a predetermined mathematical function on the authentication message to generate a result, to encrypt the result using the transmitter key to generate an encrypted result, and to send the encrypted result to the receiver over the channel, and the receiver is configured to generate a decrypted result by decrypting the encrypted result using the receiver key, and to determine whether the decrypted result satisfies a predetermined criterion.

71. The system of claim 70, wherein the first data is a pseudo-random value, and the receiver is configured to generate the pseudo-random value for use in generating the authentication message.

72. The system of claim 70, wherein the receiver is configured to treat the receiver key as an invalid key unless the decrypted result satisfies the predetermined criterion.

73. The system of claim 70, wherein the transmitter is configured to transmit additional data with the encrypted result over the channel to the receiver.

74. The system of claim 73, wherein the additional data is key material.

75. The system of claim 70, also including a TMDS-like link between the transmitter and the receiver, wherein the protocol is a symmetric block protocol in which the transmitter sends encrypted data over the TMDS-like link to the receiver and the receiver decrypts the encrypted data in response to the receiver key and a sequence of count values, wherein the transmitter is configured to generate a pseudo-random value, the transmitter is configured to transmit the pseudo-random value over one of the communication channel and the TMDS-like link to the receiver, and the receiver is configured to include the pseudo-random value as a field of at least one of the count values upon determining that the decrypted result satisfies the predetermined criterion.

76. The system of claim 75, wherein the communication channel is a channel of the TMDS-like link, and wherein the transmitter is configured to transmit the pseudo-random value and the encrypted result over said channel of the TMDS-like link to the receiver.

77. The system of claim 70, also including:

an external agent configured to be coupled to each of the receiver and the transmitter, wherein the external agent is configured to provide the transmitter key to the transmitter when coupled to said transmitter and to provide the receiver key to the receiver when coupled to said receiver.

78. A method for implementing a content protection protocol using a transmitter, a receiver, and a communication link between the transmitter and the receiver, said method including the steps of:

(a) providing a receiver key to the receiver and providing a transmitter key to the transmitter;

(b) operating the transmitter and the receiver to perform a challenge-response procedure to determine whether at least one of the transmitter key and the receiver key satisfies a predetermined criterion, thereby determining whether the receiver key has a predetermined relationship to the transmitter key; and

(c) upon determining that said at least one of the transmitter key and the receiver key satisfies the predetermined criterion, enabling the receiver to use the receiver key to decrypt data received over the link.

79. The method of claim 78, wherein step (b) includes the step of determining whether the transmitter key matches the receiver key.

80. The method of claim 78, wherein step (b) includes the steps of:

(d) operating the receiver to encrypt first data in accordance with the protocol using the receiver key to generate an authentication message;

(e) sending the authentication message to the transmitter;

(f) operating the transmitter to perform a predetermined mathematical function on the authentication message to generate a result, and to encrypt the result using the transmitter key to generate an encrypted result;

(g) sending the encrypted result to the receiver;

(h) operating the receiver to generate a decrypted result by decrypting the encrypted result using the receiver key; and

(i) determining from the decrypted result whether said at least one of the transmitter key and the receiver key satisfies the predetermined criterion.

81. The method of claim 80, wherein the transmitter is configured to transmit additional data with the encrypted result to the receiver, said method also including the step of:

(j) upon determining that said at least one of the transmitter key and the receiver key satisfies the predetermined criterion, operating the receiver in response to said additional data.

82. The method of claim 81, wherein the additional data is key material.

83. The method of claim 80, wherein the first data is a pseudo-random value, and step (d) includes the steps of generating the pseudo-random value and encrypting the pseudo-random value in accordance with the protocol using the receiver key to generate the authentication message.

84. The method of claim 80, wherein the protocol is a symmetric block protocol in accordance with which the transmitter can send encrypted data over the link to the receiver and the receiver can decrypt the encrypted data in response to the receiver key and a sequence of count values, wherein step (b) also includes the steps of:

operating the transmitter to generate a pseudo-random value; and

sending the pseudo-random value to the receiver,

and wherein step (c) includes the step of including the pseudo-random value as a field of at least one of the count values upon determining that said at least one of the transmitter key and the receiver key satisfies the predetermined criterion.

85. The method of claim 78, wherein step (c) includes the step of:

preventing the receiver from using the receiver key to decrypt data received over the link unless said at least one of the transmitter key and the receiver key satisfies the predetermined criterion.

86. The method of claim 78, wherein step (a) includes the step of:

coupling an external agent to the receiver and sending, from the external agent to the receiver, at least one of the receiver key, an encrypted version of the receiver key, and data enabling the receiver to obtain the receiver key.

87. The method of claim 78, wherein the link is a TMDS-like link, and wherein step (a) includes the step of:

coupling an external agent to the receiver and sending, from the external agent to the receiver, at least one of the receiver key, an encrypted version of the receiver key, and data enabling the receiver to obtain the receiver key.